ABSTRACT

A method and system for booting up a computer system in a secure fashion is disclosed. The method and system comprise determining the presence of a security feature element during an initialization of the computer system wherein the security feature element includes a public key and a corresponding private key, storing a portion of the public key in a nonvolatile memory within the computer system if the security feature element is present and utilizing an algorithm to determine the presence of the security feature element prior to a subsequent boot-up of the computer system. Through the use of the present invention, a computer system is capable of being booted up whereby the computer system determines if a security feature element was previously present in the system. If a security feature element was previously present in the computer system, any stored keys, along with the secrets that they protect, are prevented from being compromised. It is also an object of the present invention to preclude the system from compromising any keys and associated secrets if a security feature element in the system was not previously present in the system.